

Neutrosophic Computing and Machine Learning {Número especial: Neutrosofía: Herramienta para investigación y toma de decisiones en ambientes de indeterminación}, Vol. 30, 2023

University of New Mexico



# Análisis estadístico neutrosófico sobre ciberriesgos de los estudiantes universitarios basado en la utilización de redes sociales.

# Neutrosophic statistical analysis on cyber risks of university students based on social network usage.

**Luz Marina Aguirre Paz [1], Fausto Alberto Viscaino Naranjo [2], and Angela Karina Bustillos Mallitasig [3]**

[1] Universidad Regional Autónoma de Los Andes, Ambato. Ecuador. **E-mail:** ua.luzaguirre@uniandes.edu.ec
[2] Universidad Regional Autónoma de Los Andes, Ambato. Ecuador. **E-mail:** ua.faustoviscaino@uniandes.edu.ec
[3] CiberSec , Latacunga. Ecuador. **E-mail:** angela.bustillos27@gmail.com

**Resumen**. La presente investigación conlleva a los estudiantes universitarios a conocer los ciberriesgos a los que están expuestos mediante el uso constante de las redes sociales; algunos de los riesgos más comunes incluyen la exposición de información personal, el acoso en línea, la ciber extorsión, el robo de identidad y la propagación de malware a través de mensajes de phishing y otros ataques cibernéticos. Los estudiantes universitarios pueden ser especialmente vulnerables debido a su relativa inexperiencia en el uso de las redes sociales y su tendencia a compartir información personal en línea. El objetivo de la investigación es realizar un análisis estadístico neutrosófico sobre ciberriesgos de los estudiantes universitarios basado en la utilización de redes sociales. En la investigación se siguió los postulados de los estudios no experimentales de tipo transversal y descriptivo. Donde se seleccionaron un conjunto de métodos y técnicas tanto teóricos, como empíricos y matemáticos estadísticos. Los que permitieron realizar una recopilación de datos de diversas fuentes y que con la ayuda de un algoritmo neutrosófico se logró obtener resultados más robustos. Todo lo antes planteado le ofrece un alto nivel de validez a los resultados obtenidos en esta investigación.

**Palabras clave:** estadística neutrosófica, ciberseguridad, ciberriesgos,redes sociales, ciber extorsión

**Summary.** The present research leads college students to be aware of the cyber risks to which they are exposed through their constant use of social networks; some of the most common risks include exposure of personal information, online harassment, cyber extortion, identity theft, and the spread of malware through phishing messages and other cyber attacks. College students may be especially vulnerable due to their relative inexperience in using social networks and their tendency to share personal information online. The objective of the research is to conduct a neutrosophical statistical analysis on cyber risks of college students based on the use of social networks. The research followed the postulates of non-experimental studies of cross-sectional and descriptive type. A set of theoretical, empirical and mathematical statistical methods and techniques were selected. These allowed the collection of data from different sources and with the help of a neutrosophic algorithm, it was possible to obtain more robust results. All of the above offers a high level of validity to the results obtained in this research.

**Keywords:** neutrosophic statistics, cybersecurity, cyber risks, social networks, cyber extortion

## 1 Introducción

Actualmente las relaciones sociales han innovado con la aplicación de las tecnologías de información y comunicación. Existen un gran número de redes sociales de acceso libre en internet, donde cualquier cibernauta puede crear una cuenta, configurar un perfil con información personal auténtica o ficticia y acceder a un mundo de comunicaciones e interacciones con amigos, familiares, compañeros o simplemente relacionarse con usuarios completamente desconocidos que cuenten con un perfil dentro de una red social como Facebook, convirtiéndose sin lugar a dudas en el instrumento favorito para el contacto e intercambio de experiencias, [1].

Las redes sociales son aplicaciones que admiten la participación en un espacio común en torno a intereses compartidos, necesidades y objetivos comunes de colaboración, intercambio de conocimientos, interacción y comunicación, [2].

La característica principal de las redes sociales es que permiten al usuario final acceder, crear, difundir y compartir información fácilmente en un entorno abierto y sencillo de usar; por lo general, el único costo es el tiempo del usuario final. A menudo, existen pocos controles sobre el contenido, además de los impuestos normalmente por un estado o gobierno (como la difamación o la pornografía), o cuando existen controles, los imponen los propios usuarios, [3].

El concepto de red social es muy complejo, por lo que resulta realmente complicado desarrollar una acepción unívoca debido a la gran diversidad de usos y la heterogeneidad de las investigaciones y marcos teóricos en los que ha sido utilizada, [4].

Las redes sociales se incorporaron de manera importante en nuestra vida, de modo que se encuentran presentes en todos los ámbitos, incluso aquellas personas que no cuentan con un una laptop, celular, al menos, han escuchado de ellas. Las redes sociales son plataformas en línea que permiten a los usuarios conectarse y compartir información con otros usuarios. Estas plataformas suelen incluir características como perfiles de usuario, funciones de mensajería y publicaciones de noticias, hay muchas redes sociales populares en todo el mundo, como Facebook, Instagram, Twitter, LinkedIn, TikTok, Snapchat y Whatsapp, cada una con su propia audiencia y estilo de uso. Estas redes sociales son utilizadas por una amplia variedad de personas, desde jóvenes hasta personas mayores, desde individuos hasta empresas y organizaciones.

En Ecuador, las redes sociales son muy populares y ampliamente utilizadas por la población en general, algunas de las redes sociales más populares en el país son Facebook, Whatsapp, Instagram, Twitter, Tiktok y Youtube, cada una de estas plataformas tienen diversas funciones y son utilizadas diariamente. Además de estas redes sociales, también hay algunas redes sociales populares en Ecuador que están orientadas a comunidades específicas, como LinkedIn para profesionales y Xing para empresarios. Es importante destacar que, aunque las redes sociales tienen muchos beneficios, también hay riesgos asociados con su uso. Es necesario que los usuarios de redes sociales en Ecuador sean conscientes de estos riesgos y tomen medidas de seguridad adecuadas para proteger su información personal y su privacidad, [5-23].

Las redes sociales son una herramienta popular entre los estudiantes universitarios para conectarse con sus compañeros de clase, comunicarse con sus profesores y para mantenerse informados sobre eventos y noticias relacionadas con la universidad; sin embargo, su uso puede tener tanto beneficios como riesgos.

Algunos de los beneficios del uso de las redes sociales por los estudiantes universitarios son: 1) Conexión social, permite a los estudiantes conectarse con otros estudiantes que comparten las mismas aficiones e intereses, lo que ayuda a crear un sentido de comunidad en el campus universitario. 2) Comunicación con los docentes, las redes sociales ayudan a los estudiantes a comunicarse con los docentes de una manera fácil e informal. 3) Acceso a información y noticias, los estudiantes pueden usar las redes sociales para mantenerse informados de los acontecimientos relacionados con la universidad y su comunidad social. 4) Desarrollo profesional, las redes sociales pueden ser una herramienta útil para los estudiantes que buscan establecer contactos con profesionales en su campo de interés y establecer conexiones que puedan ayudarles en su carrera profesional.

Para reducir los riesgos cibernéticos, los estudiantes universitarios deben ser conscientes de las amenazas potenciales y tomar medidas de seguridad adecuadas, como mantener sus perfiles en redes sociales privados, utilizar contraseñas seguras, evitar descargar software de fuentes no confiables y utilizar software de seguridad adecuado en sus dispositivos.

Los diversos aspectos del uso, el abuso del internet y de los dispositivos digitales relacionados están ahora regidos por leyes civiles y penales. Educar a los estudiantes sobre ciberseguridad debe incluir también suscitar la conciencia de los estudiantes de las consecuencias potenciales de su conducta al utilizar los sistemas informáticos y de comunicación, [6-24].

La protección de la privacidad en los entornos digitales debe ser una prioridad formativa desde diferentes instancias educativas, para que pueda convertirse no sólo en una habilidad, sino también en un valor a potenciar, [7].

La importancia de la prevención para evitar que se den situaciones de este tipo y fomentar el diálogo entre adultos y navegar sin peligro, disfrutando de la tecnología en forma segura. Una de las amenazas en las redes sociales son el ciberacoso, secuestro, trata de personas, daños a la moral, entre otras, [8-25].

Por lo consiguiente, las universidades deben preocuparse de la seguridad de los estudiantes, identificar los riesgos cibernéticos a los que están expuestos y encontrar soluciones para la protección de la confidencialidad de la información, así también precautelar la integridad de los universitarios con la implementación de buenas prácticas de ciberseguridad.

Sin embargo, el uso excesivo de las redes sociales conlleva a diversos riesgos que puede ocasionar varios daños a las personas que lo utilizan, entre ellos se puede mencionar robo de identidad, acoso en línea, pérdida de tiempo y productividad, adicción a las redes sociales, entre otras. Por lo tanto, es importante que los estudiantes universitarios utilicen las redes sociales de manera responsable y tomen medidas de seguridad adecuadas para reducir los riesgos asociados con su uso.

El acoso digital se asocia con la extensión de las nuevas aplicaciones orientadas a la comunicación, como la telefonía móvil o Whatsapp, las redes sociales como Tuenti y Facebook, los Fotolog y Web de vídeo como

Youtube, [9].

Otro tipo de ataque es el Trolling, se refiere a los usuarios que responden en las redes sociales con publicaciones y comentarios inventados, para provocar un aumento en los usuarios [10], Por lo consiguiente, (DiResta et al., 2019) señalan que un actor malicioso interesado en trollear busca "empujar" opiniones sobre temas polarizantes o controvertidos a través de las redes sociales.

Los argumentos antes panteados permiten identificar el siguiente problema de investigación ¿Cómo valorar desde un enfoque neutrosófico los ciberriesgos de los estudiantes universitarios basado en la utilización de redes sociales?

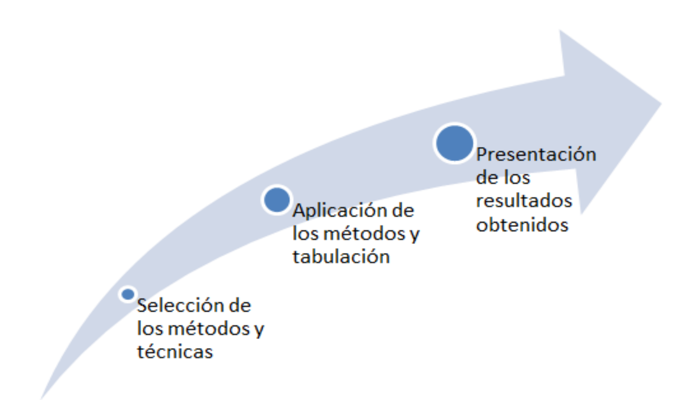
Es por ello que, la presente investigación tiene como objetivo: realizar un análisis estadístico neutrosófico sobre ciberriesgos de los estudiantes universitarios basado en la utilización de redes sociales.

## 2 Materiales y métodos

Se realizó una investigación mixta: "Los métodos mixtos o híbridos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos tanto cuantitativos como cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada", [11-26].

Dentro de ellos se siguieron los postulados de los estudios no experimentales de tipo transversal y descriptivo. Según recomendaciones del autor antes mencionados. Por lo que se siguen los posos presentados en el diagrama 1.

**Diagrama 1.** Momento del estudio transversal descriptivo realizado




A continuación se presentan los métodos y técnicas utilizados en la investigación. Los cuáles serán descritos en correspondencia con las características de la investigación desarrollada.

**Teóricos**

Analítico-sintético: permitió realizar un estudio acerca del estado del arte sobre ciberriesgos de los estudiantes universitarios basado en la utilización de redes sociales. Se empleó para la sistematización, generalización y concreción de la información procesada. Fue útil en la interpretación de la información empírica obtenida.

Inductivo-deductivo: posibilitó hacer inferencias sobre el análisis estadístico neutrosófico sobre ciberriesgos de los estudiantes universitarios basado en la utilización de redes sociales, así como la interpretación de los datos obtenidos, a partir de las cuales se deducen nuevas conclusiones lógicas.

**Empíricos**

Revisión de documentos como: se revisaron diferentes artículos científicos y sitios de internet se realizan encuestas enfocadas al uso de las redes sociales, uso del celular y los riesgos a los que están expuestos. A su vez, se puede palpar que el mayor índice de acosos en línea, ciberbullying entre otros, son los niños, jóvenes y adolescentes, ellos son los más vulnerables por que no conocen de los riesgos cibernéticos, de la misma manera se menciona que uno o dos miembros de la familia o amigos han sido víctimas de fraude en línea y robo de información o ciber extorción.

**Estadísticos matemáticos**

Se emplea la estadística descriptiva, de manera general y el caso particular de el análisis de distribución de frecuencias absolutas y realativas. Además, se confeccionar gráficos de barras para una mayor ilustración de los resultados presentados.

### 2.1 Población y muestra

La población de estudio corresponde a los ecuatorianos que tienen edades comprendidas entre 18 y 24 años de edad, siendo así el 12,1% de la población ecuatoriana, con las proyecciones censales de población por edades realizada por el Instituto Nacional de Estadísticas y Censos INEC, teniendo una cifra de 2.152.890 personas, [12].

Para contextualizar el artículo, se desarrolla procesos de búsqueda selectiva de información en libros, artículos científicos, revistas y sitios de internet; para fundamentar el objeto de estudios de la presente investigación, para fundamentar el objeto de estudios de la presente investigación se extraen los datos de la realidad, utilizando técnicas de recolección de datos existentes en el que se tiene como referencia los índices de uso de internet y uso de redes sociales, cada una de las estadísticas ayuda a que se tenga un contexto claro de los ciberriesgos que cada usuario activo mantiene a diario por el desconocimiento del mismo.

En las diferentes búsquedas selectivas se pudo evidenciar que existe un alto índice de uso de redes sociales, no solamente para publicaciones y compartir información; si no también que se utiliza para medios de marketing, publicidad y ámbitos educativos.

### 2.2 Método neutrosófico

El método neutrosófico es un enfoque lógico y filosófico desarrollado por el matemático y filósofo rumano-francés Florentin Smarandache a fines del siglo XX. Este método se utiliza para abordar situaciones en las cuales la verdad, la falsedad y la indeterminación coexisten de manera simultánea.

La idea fundamental detrás del método neutrosófico es la introducción de un tercer componente llamado "indeterminación", además de verdad y falsedad, para describir fenómenos en los cuales la información disponible es incompleta o incierta. Así, se reconoce que no todas las afirmaciones pueden ser clasificadas inequívocamente como verdaderas o falsas; algunas pueden estar en un estado indeterminado.

El método neutrosófico ha sido aplicado en diversas áreas, como la inteligencia artificial, la toma de decisiones, la teoría de conjuntos, la lógica, y la filosofía en general. Proporciona un marco para analizar y modelar la incertidumbre de manera más completa que los sistemas lógicos clásicos que solo considera la verdad y la falsedad [13-27].

Para el análisis neutrosófico desarrollado se tuvo en cuenta el flujo de trabajo de 6 activiadades lógicas (Diagrama 2), tenidos en cuenta para desarrollar la investigación, con su respectiva explicación. El análisis se basa en el funcionamiento del entorno neutrosófico para modelar la incertidumbre. El análisis se sustenta sobre una guía de pasos lógicas con enfoque neutrosófico que puede abordar criterios de diferente naturaleza en un entorno neutrosófico [14], [15-28], [16-29].

**Diagrama 2.** Flujo de actividades en el entorno neutrosófico realizado en la investigación



## 3 Resultados y discusión

América Latina está cada vez más en riesgo de ser el blanco principal para los agresores cibernéticos, tanto las cifras de los ciudadanos como las cifras de los usuarios conectados al internet van en aumento.

Ecuador es un país con 18 millones de habitantes, de los cuales el 77% son usuarios de Internet hay 15.91 millones de celulares en el país y 81% de la población es usuaria activa en redes sociales, es decir, hay más perfiles

en redes sociales que usuarios conectados diariamente a Internet.

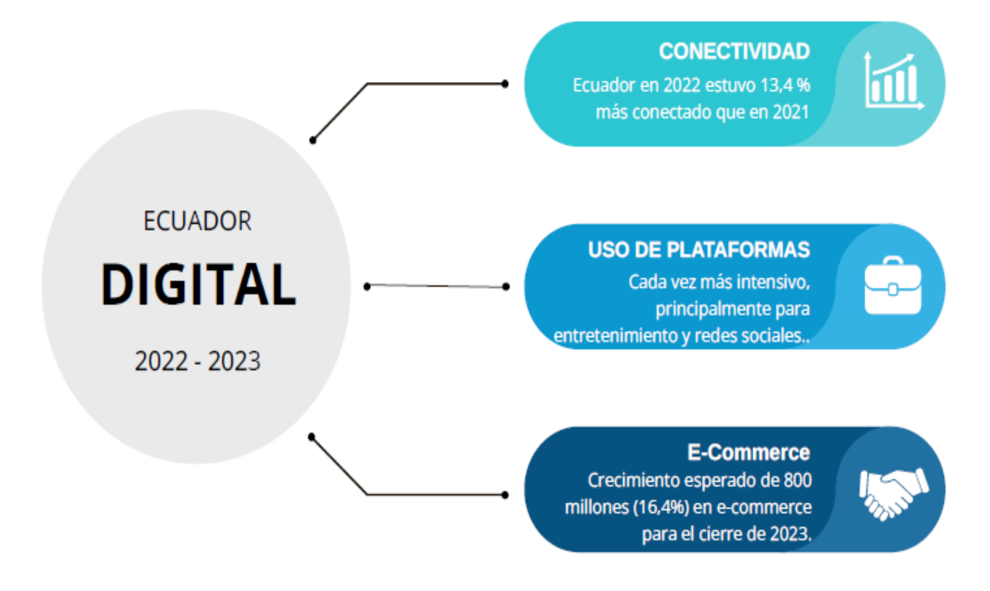
**Figura 1.** Crecimiento digital en Ecuador



**Fuente:** Medina, [17]

Ecuador hoy tiene un 13,4% más de conexiones que en 2021 ya que ha realizado millones de dólares más en transacciones y se espera que este crecimiento continúe, esperándose $800 millones adicionales en comercio electrónico (16,4%) al cierre del 2023.

**Figura 2.** Cifras Ecuador digital 2022-2023




**Fuente:** Alcazar Ponce, [18]

El 76% de la población usa internet activamente, tanto para búsquedas, así como acceso a las redes sociales, por su parte, el 98% de usuarios acceden a las redes sociales mediante su celular siendo así el dispositivo móvil la herramienta principal de conexión para ingresar a Instagram, Facebook, Tik Tok entre otras redes sociales.

**Figura 3.** Uso de internet




**Fuente:** Medina, [17]

Con los datos obtenidos se puede observar que el crecimiento de usuarios en las redes sociales ha incrementado notablemente desde enero 2021 a enero 2022, con el 75% Pinterest es la red social más usada por los usuarios, seguida de Tik Tok con el 74%.

**Figura 4.** Crecimiento de Usuarios de Redes Sociales




**Fuente:** Alcazar Ponce, [18]

WebSide realizó una infografía de la red social más conocida Facebook, en el cual determina que el 54% son cuentas duplicadas seguidas del 18% de cuentas spam y el 28% son cuentas de usuarios mal clasificados.

**Figura 5.** Cuentas Falsas

## 4 Discusión

El 81% de los usuarios a nivel del Ecuador son usuarios activos en las redes sociales, por lo consiguiente es necesario conocer los riesgos que existen al momento de crear perfiles en las diferentes redes sociales, leer claramente las políticas de privacidad que cada una de las redes sociales establecen al momento de registrar los datos personales.

Los resultados obtenidos demuestran que el 76% de la población usa internet activamente para ingresar a las redes sociales, esto quiere decir que la gran mayoría de la población no conoce los riesgos que puede ocasionar la publicación de información personal en las diferentes redes sociales.

Kevin Mitnick en su libro "The Art of Invisibility", el experto en seguridad cibernética explica cómo los atacantes pueden utilizar las redes sociales para obtener información personal de los usuarios y utilizarla para comprometer su seguridad, [19].

La consultora en seguridad cibernética, Symantec, ha señalado que los ataques de ingeniería social son cada vez más sofisticados, y que los atacantes utilizan las redes sociales para recopilar información personal y de inteligencia para dirigir sus ataques, [20].

El experto en seguridad Scott Schober, en su libro "Hacked Again", argumenta que la mayoría de los ataques cibernéticos son el resultado de la falta de conciencia y educación en ciberseguridad por parte de los usuarios, lo que incluye el uso inadecuado de las redes sociales, [21].

Cada uno de los autores manifiestan que están de acuerdo en que las redes sociales son un objetivo común para los ciberataques, y que los usuarios deben ser conscientes de los riesgos y tomar medidas de seguridad adecuadas para protegerse a sí mismos y a su información personal.

Así mismo, con base a la revisión realizada sobre las dimensiones vinculadas a la seguridad y protección de datos donde Ecuador ocupa el sexto lugar en ciberseguridad en América latina [22] , para protegerse en línea y reducir los ciberriesgos en las redes sociales, aquí hay algunas medidas de ciberseguridad que se pueden considerar:

Uso de contraseñas seguras: Use una contraseña única y segura para cada cuenta de redes sociales. Las contraseñas seguras deben ser largas y contener una combinación de letras, números y caracteres especiales.

Configurar la privacidad: Revisar la configuración de privacidad de las cuentas de redes sociales y ajustarlas de acuerdo a las preferencias personales. Es importante limitar la cantidad de información personal que se comparte públicamente y asegurarse de que solo se comparte con personas de confianza.

Desconfiar de mensajes desconocidos: Tener precaución al hacer clic en enlaces o descargar archivos de mensajes desconocidos en las redes sociales. Es importante verificar la fuente del mensaje antes de tomar cualquier acción.

Evitar el uso de Wi-Fi público no seguro: Evitar conectarse a Wi-Fi público no seguro al usar las redes sociales, esto puede exponer la información personal a posibles piratas informáticos.

Mantener el software actualizado: Mantener el software de las redes sociales y del dispositivo actualizado para asegurarse de que se estén utilizando las últimas medidas de seguridad.

No compartir información personal: Evitar compartir información personal, como números de teléfono, direcciones de correo electrónico o direcciones físicas, en las redes sociales.

Configurar la autenticación de dos factores: Configurar la autenticación de dos factores para las cuentas de redes sociales, esto da añadir una capa adicional de seguridad al necesitar un código adicional para el inicio de sesión en las diferentes cuentas de las redes sociales.

Al seguir estas medidas de ciberseguridad se puede reducir los ciberriesgos asociados con el uso de las redes sociales y proteger la información personal en línea de los estudiantes universitarios.

## Conclusiones

El alto crecimiento de popularidad de las redes sociales ocasiona que estos sitios se conviertan en el principal centro de ataque de cibercriminales, lo que conlleva a estar más prevenidos en cuanto a la seguridad y privacidad de la información que se compartimos en las diferentes plataformas.

Actualmente los ciberriesgos en las redes sociales van aumentando y presentan una vulneración mayor para los estudiantes universitarios, quienes son los principales consumidores de estas plataformas; por esta razón, se debe tomar medidas de seguridad respecto a la información las mismas que permita proteger la integridad de cada uno de los usuarios.

Los resultados obtenidos en la investigacion con la vinculación de la estadística clásica y la neutrosófica denotan una validez importante, pero a su vez dejan temáticas abiertas para futuros estudios para futuras investigaciones donde existan manipulación de las variables.

## Referencias

[1] F. G. Jara Obregón Luis. Delitos a través redes sociales en el Ecuador: una aproximación a su estudio. I+D Tecnológico, 113-114, 2017

[2] W Pettenati, & K Tochtermann. Innovative Approaches for Learning and Knowledge Sharing: First European Conference on Technology Enhanced Learning, EC-TEL 2006 Crete, Greece, October 1-4, 2006 Proceedings (Vol. 4227). Springer Berlin Heidelberg. https://doi.org/10.1007/11876663, 2006

[3] A. W Bates & A. W Bates. *7.6 Social media*. https://opentextbc.ca/teachinginadigitalage/chapter/9-5-5-social-media/, 2015

[4] A. Cea Jiménez. Los delitos en las redes sociales: Aproximación a su estudio y clasificación. https://gredos.usal.es/handle/10366/121119, 2012

[5] W. E Martínez Chérrez, & D. F Avila Pesantez. Ciberseguridad en las redes sociales: Una revisión teórica. Revista UNIANDES Episteme, 8(2), 211-234, 2021

[6] N Giant. Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones. Narcea Ediciones, 2016

[7] M. J Hernandez-Serrano, P Renés-Arellano, R Campos Ortuño, & B González-Larrea. Privacidad en redes sociales: Análisis de los riesgos de auto-representación digital de adolescentes españoles. Revista Latina de Comunicación Social, 79, 133-154. https://doi.org/10.4185/RLCS-2021-1528, 2021

[8] A. P Aguilar. Las redes sociales y sus factores de riesgos. Pro Sciences: Revista de Producción, Ciencias e Investigación, 10-13, 2017

[9] C. S Fernández, & L. L Hernáez. Factores de riesgo en el Ciberbullying. Frecuencia y exposición de los datos personales en Internet. International Journal of Sociology of Education, 4(1), Article 1. https://doi.org/10.4471/rise.2015.01, 2015

[10] F. G. Galay. Hola. Llueve. Libertad de expresión, trolling y la absurda lógica de la circulación en redes, 2018

[11] R Hernández-Sampierire. Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta, 10. https://doi.org/978-1-4562-6096-5, 2018

[12] INEC. *Proyecciones Poblacionales*. Instituto Nacional de Estadística y Censos. Recuperado 2 de abril de 2023, de https://www.ecuadorencifras.gob.ec/proyecciones-poblacionales/, s. f

[13] Smarandache, F., Neutrosophic set–a generalization of the intuitionistic fuzzy set. Journal of Defense Resources Management (JoDRM), 2010. 1(1): p. 107-116

[14] O. Mar, I. Santana, and J. Gulín, "Algoritmo para determinar y eliminar nodos neutrales en Mapa Cognitivo Neutrosófico," Neutrosophic Computing and Machine Learning, vol. 8, pp. 4-11, 2019.

[15] R. G. Ortega, M. Rodríguez, M. L. Vázquez, and J. E. Ricardo, "Pestel analysis based on neutrosophic cognitive maps and neutrosophic numbers for the sinos river basin management," Neutrosophic Sets and Systems, vol. 26, no. 1, pp. 16, 2019.

[16] S. A., Edalatpanah, & Smarandache, F. (2019). Data envelopment analysis for simplified neutrosophic sets. Infinite Study.

[17] K. R Medina. Estadísticas de la situación Digital en Ecuador 2021-2022. *Branch Agencia*. https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-en-ecuador-2021-2022/, 2022

[18] J. P Alcazar Ponce. Estado Digital Ecuador 2022—Estadísticas Digitales. *Mentinno - Formacion Gerencial Blog*. https://blog.formaciongerencial.com/estado-digital-ecuador-2022-estadisticas-digitales/, 2022

[19] K. D Mitnick, R Vamosi, & M Hypponen. The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of Big Brother and big data. Back Bay Books / Little, Brown and Company, 2019.

[20] Conzultek. *Symantec: El servicio integral de protección de datos ante amenazas avanzadas*. Recuperado 2 de abril de 2023, de https://blog.conzultek.com/ciberseguridad/symantec-el-servicio-de-proteccion-de-datos, s. f

[21] M.-L Kamberg. Ciberseguridad: Protege tu identidad y tus datos (Cybersecurity: Protecting Your Identity and Data). The Rosen Publishing Group, Inc, 2017

[22] MINTEL. *Índice de Ciberseguridad*. https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/, 2023

[23] Estupiñan Ricardo, J., Romero Fernández, A. J., & Leyva Vázquez, M. Y. ¨Presencia de la investigación científica en los problemas sociales post pandemia¨. Conrado, vol 18 núm 86, pp 258-267, 2022. http://scielo.sld.cu/pdf/rc/v18n86/1990-8644-rc-18-86-258.pdf

[24] Estupiñán Ricardo, J., Leyva Vázquez, M. Y., Marcial Coello, C. R., & Figueroa Colin, S. E. ¨Importancia de la preparación de los académicos en la implementación de la investigación científica¨. Conrado, vol 17 núm 82, pp 337-343, 2021. http://scielo.sld.cu/pdf/rc/v17n82/1990-8644-rc-17-82-337.pdf

[25] Ramos Sánchez, R. E., Ramos Solorzano, R. X., & Estupiñán Ricardo, J. ¨La transformación de los objetivos de desarrollo sostenible desde una dinámica prospectiva y operativa de la Carrera de Derecho en Uniandes en época de incertidumbre¨. Conrado, vol 17 núm 81, pp 153-162, 2021. http://scielo.sld.cu/pdf/rc/v17n81/1990-8644-rc-17-81-153.pdf

[26] Falcón, V. V., Quinapanta, M. D. R. A., Villacís, M. M. Y., & Ricardo, J. E. ¨Medición del capital intelectual: Caso hotelero¨. Dilemas Contemporáneos: Educación, Política y Valores, 2019.

[27] Leyva Vázquez, M. Y., Viteri Moya, J. R., Estupiñán Ricardo, J., & Hernández Cevallos, R. E. ¨Diagnosis of the challenges of post-pandemic scientific research in Ecuador¨. Dilemas contemporáneos: educación, política y valores, vol 9 núm (spe1), 2021. https://www.scielo.org.mx/pdf/dilemas/v9nspe1/2007-7890-dilemas-9-spe1-00053.pdf

[28] Gómez, G. A. Á., Vázquez, M. Y. L., & Ricardo, J. E. ¨Application of Neutrosophy to the Analysis of Open Government, its Implementation and Contribution to the Ecuadorian Judicial System¨. Neutrosophic Sets and Systems, vol 52, pp 215-224, 2022.

[29] Estupiñán Ricardo, J., Martínez Vásquez, Á. B., Acosta Herrera, R. A., Villacrés Álvarez, A. E., Escobar Jara, J. I., & Batista Hernández, N. ¨Sistema de Gestión de la Educación Superior en Ecuador. Impacto en el Proceso de Aprendizaje¨. Dilemas Contemporáneos: Educación, Política y Valores, 2018. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/321/808

**Recibido:** Septiembre 25, 2023. **Aceptado:** Octubre 18, 2023